UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/581,064	10/07/2002	Ahmet Mursit Eskicioglu	RCA88783	6883

24498 7590 03/03/2008

Joseph J. Laks
Thomson Licensing LLC
2 Independence Way, Patent Operations
PO Box 5312
PRINCETON, NJ 08543

EXAMINER	
PATEL, NIRAV B	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
03/03/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/581,064	ESKICIOGLU ET AL.	
	Examiner	Art Unit	
	NIRAV PATEL	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 December 2007 (Amendment)*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,8 and 9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 2* is/are rejected.

7)☒ Claim(s) *3,4,8 and 9* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's amendment filed on Dec. 07, 2007 has been entered. Claims 1-4, 8 and 9 are pending. Claims 1 and 3 are amended and Claims 8 and 9 are newly added by the applicant.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Matsumoto et al (US Patent No. 5,351,294) in view of Takaragi et al (US Patent No. 5,103,479) and in view of Elteto et al (US Patent No. 5,737,424).

As per claim 1, Matsumoto teaches:

receiving said signal in a smart card, said signal being scrambled using a scrambling key [Fig. 1, 4, 5, col. 6 lines 58-68]; receiving, in said smart card, data representative of a first seed value [Fig. 4, 5, col. 7 lines 20-45]; (c) generating, in said smart card, said scrambling key using said first seed value and a second seed value in a predetermined function, whereby secret sharing is implemented, said second seed value being permanently stored in said smart card [Fig. 4, 5, 7A, 7B, col. 7 lines 24-49, col. 4 lines 40-45].

Matsumoto teaches descrambling said signal using said generated scrambling key to provide a descrambled signal [col. 7 lines 5-7, Fig. 4].

Matsumoto teaches a receiving station/user terminal, which further comprises the IC card and performs the descrambling process [Fig. 4, 5]. The IC card includes a CPU and a memory as shown in Fig. 7A. Matsumoto doesn't expressively mention descrambling in said smart card.

However, Takaragi teaches ciphering/deciphering equipment includes a CPU and a memory and performs the ciphering/deciphering operation [Fig. 1, col. 5 lines 36-52]. Further, Takaragi teaches the IC card includes a microcontroller and a memory, which performs the same function as the CPU (i.e. ciphering/deciphering operation) [col. 10 lines 25-29, Fig. 10 i.e. descrambling in said smart card].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Takaragi and Matsumoto, since one would have been motivated to provide the enciphering/deciphering function at a high seed [Takaragi, col. 3 lines 25-33] and reduce a load/burden on the whole system/broadcast function [Matsumoto, col. 4 lines 5-6].

Matsumoto teaches the first seed value and the second seed value for generating the scrambling key [col. 7 lines 20-49]. Matsumoto and Takaragi don't expressively mention seed value representing point in a coordinate system.

Elteto teaches the first seed value representing a first point in a coordinate system and the second seed value representing a second point in the coordinate system [col. 9 lines 24-36, col. 10 lines 12-20, 21-59].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Elteto and Takaragi and Matsumoto, since one would have been motivated to utilize elliptical curve system for encrypting and decrypting the data for a given level of security [col. 2 lines 11-16].

3. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Matsumoto et al (US Patent No. 5,351,294) in view of Takaragi et al (US Patent No. 5,103,479) and in view of Elteto et al (US Patent No. 5,737,424) and in view of Schwenk et al (US Patent No. 6,760,445).

As per claim 2, the rejection of claim 1 is incorporated and Matsumoto teaches the first and second seed values [col. 7 lines 21-48]. Elteto teaches the points (the seed values) are points on the elliptic curve [col. 9 lines 24-30].

Schwenk teaches points on a Euclidean plane [Fig. 1, 4 col. 3 lines 19-30].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Schwenk with Matsumoto, Takaragi and Elteto, since one would have been motivated to calculate a key and enhance the security in the distributed data network [Schwenk, col. 5 lines 43-50].

Response to Amendment

4. Applicant has amended claim 1, which necessitated new ground of rejection. See rejection above.

Regarding to the Applicant's argument that "Matsumoto does not disclose or suggest a second seed value permanently stored in the smart card", Examiner disagrees with applicant, since Matsumoto discloses the internal structure of the IC card as shown in Fig. 7A, which includes a CPU, memory ...etc. The term initial values 706, 707, 708...are the initial value assigned to respective terms of the effective period of the IC card and are used for generating a hash total (i.e. values are stored in the memory of the IC card) [col. 9 lines 6-9, Fig. 7A]. Further, the term initial value for the read-out present time is used as the parameter k which is parameter of the hash function (i.e. the parameter or value is a seed which is used for calculating the key) [col. 6 lines 27-30, col. 7 lines 29-49]. Therefore, Matsumoto teaches the claim limitation "a second seed value permanently stored in the smart card). In this case, the combination of Matsumoto, Takaragi and Elteto discloses the amended claim limitation as above.

Allowable Subject Matter

5. Claims 3, 4, 8 and 9 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Moerder (US 4634808) – Descrambler subscriber key production system utilizing key seeds stored in descrambler

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nirav Patel whose telephone number is 571-272-5936. If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kim Vu can be reached on 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

/Thanhnga B. Truong/

Primary Examiner, Art Unit 2135

NBP

2/21/08